

REMARKS

This Application has been carefully reviewed in light of the Office Action mailed on March 27, 2006 (“Office Action”). Claims 1-37 and 39 are pending in the Application. Claims 1-37 and 39 were rejected in this Office Action.

Rejections Under 35 U.S.C. § 103(a):

Claims 1-6, 8, 10, 11, 13-18, 28 and 31-34 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,279,113 issued to Vimal Vaidya (“*Vaidya*”) in view of U.S. Patent No. Re 36,417 issued to Alan S. Perelson, et al. (“*Perelson*”). Claims 7 and 9 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,279,113 issued to Vimal Vaidya (“*Vaidya*”) in view of U.S. Patent No. Re 36,417 issued to Alan S. Perelson, et al. (“*Perelson*”), further in view of U.S. Patent No. 5,557,742 issued to Smaha, et al (“*Smaha*”). Claims 12 and 29 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,279,113 issued to Vimal Vaidya (“*Vaidya*”) in view of U.S. Patent No. Re 36,417 issued to Alan S. Perelson, et al. (“*Perelson*”), further in view of U.S. Patent No. 6,484,315 issued to Kavin J. Ziese (“*Ziese*”). Claim 30 was rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,279,113 issued to Vimal Vaidya (“*Vaidya*”) in view of U.S. Patent No. Re 36,417 issued to Alan S. Perelson, et al. (“*Perelson*”), further in view of U.S. Patent No. 6,484,315 issued to Kavin J. Ziese (“*Ziese*”), further in view of U.S. Patent No. 5,557,742 issued to Smaha, et al (“*Smaha*”). Applicants respectfully traverse these rejections.

Independent Claim 1 is allowable because *Vaidya* and *Perelson*, even when combined, fail to disclose, expressly or inherently “generating, for each of the one or more signature definitions, an inspector instance based on the data file” and “executing, for each of the one or more signature definitions, the generated inspector instance to detect network traffic matching the signature definition.” The Office Action concedes that *Vaidya* did not disclose the above limitations. *See* Office Action, Page 3. Rather, the Office Action points to *Perelson*’s Col. 6, lines 6-24 and Col. 8 lines 12-53, citing a test string 112 as the inspector instance. However, this is incorrect. As previously indicated in a prior response, Col 6, lines 6-24 are formulas as follows:

10

$$N_R = \frac{\ln P_f}{\ln(1 - P_M)}$$

since f is approximately $e^{-P_M^N}S = (1 - P_M)^N S$

15

$$-P_M N_S = N_S \ln(1 - P_M)$$

or

$$-P_M N_S = N_S \ln(1 - P_M)$$

or

20

$$N_R = \frac{\ln P_f}{-P_M} = \frac{-\ln P_f}{P_M}$$

Certainly, nothing is provided in these formulas which would disclose the above limitations. Additionally, the PTO has not provided any indication of their significance to the claims – other than a mere citation to them.

In the present Office Action, the PTO did not respond to Applicants' previous argument that the above formulas did not disclose the above limitations. Rather, the PTO cited a new portion of *Perelson*: Col. 8 lines 12-53, citing a test string 112 as the inspector instance. However, this is incorrect also. Col. 8, lines 12-53, indeed, describe a test string 112. However, the section immediately preceding the section cited by the PTO indicates: "The computer upon which the method of the present invention is operating generates a random test string 112." See Column 8, lines 1-3 (Emphasis added). Given that the test string 112 is randomly generated, such a test string could not disclose an inspector instance, which is generated based on a data file. Specifically, the discussion associated with the random test string 112 certainly could not disclose generating, for each of the one or more signature definitions, an inspector instance based on the data file, let alone executing, for each of the one or more signature definitions, the generated inspector instance to detect network traffic matching the signature definition. For at least this reason, Independent Claim 1 and its dependents should be allowed.

Independent Claim 11 is allowable because *Vaidya* and *Perelson*, even when combined, fail to disclose, expressly or inherently "automatically generating, for each of the one or more signatures defined in the default signature file, executable code operable to detect intrusions associated with the default signature" and "automatically generating, for each of the custom signatures, executable code operable to detect intrusions associated with the custom signature." The Office Action concedes that *Vaidya* did not disclose the above limitations. See Office Action, Page 4. Rather, the Office Action points to *Perelson* at Col 3,

lines 5-24, but this is incorrect. Col. 3, lines 5-24 describes a generation of a random test string 12 – not executable code. Accordingly, this portion of *Pereleson* clearly could not disclose the above limitations. For at least this reason, Independent Claim 11 and its dependents should be allowed.

Independent Claim 28 is allowable because *Vaidya* and *Perelson*, even when combined, fail to disclose, expressly or inherently “wherein each network detection engine is operable to generate an executable code based on either one of the stored default signatures or one of the stored user-defined signatures.” The Office Action concedes that *Vaidya* did not disclose the above limitations. *See* Office Action, Page 5. Rather, the Office Action points to *Perelson*'s Col 6, lines 6-24, but this is incorrect. The full recitation to Col 6, lines 6-24 is provided above. Col 6, lines 6-24 only includes formulas – nothing else. Certainly, these formulas do not disclose generating an executable code based on either one of the stored default signatures or one of the stored user-defined signatures. For at least this reason, Independent Claim 28 and its dependents should be allowed.

Claims 19-27 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,960,170 issued to Eva Chen, et al. (“*Chen*”), in view of U.S. Patent No. 6,725,377 issued to Kouznetsov (“*Kouznetsov*”). Applicants respectfully traverse these rejections.

Independent Claim 19 is allowable because *Chen* and *Kouznetsov*, even when combined, fail to disclose, expressly or inherently “communicating to the sensor a desire to create a modified signature from a signature to be modified” and “receiving from the sensor data indicative of parameters and associated values for the signature to be modified.” The Office Action concedes that *Chen* did not disclose the above limitations. *See* Office Action, Page 13. Rather, the Office Action points to *Kouznetsov* at Col 7, lines 39-67, but this is incorrect. Col 7, lines 39-67 generally describes attack pattern information being received at an anti-intrusion server. However, no details are given as to communicating to the sensor a desire to create a modified signature from a signature to be modified or receiving from the sensor data indicative of parameters and associated values for the signature to be modified. Lacking such details, Col. 7, lines 39-67 could not disclose the above limitations. For at least this reason, Independent Claim 19 and its dependents should be allowed.

Claims 35-37 and 39 were rejected 35 U.S.C. § 103 as being anticipated by U.S. Patent No. 6,279,113 issued to Vimal Vaidya (“*Vaidya*”) in view of U.S. Patent No.

2003/0061514 issued to Bardsley (“*Bardsley*”). Applicants respectfully traverse these rejections.

Independent Claim 35 is allowable because *Vaidya* and *Bardsley*, even when combined, fail to disclose, expressly or inherently “an engine parameter and an associated name for the engine parameter and user-defined signatures with parameter-value pairs associated with the user-defined signatures and an engine parameter and an associated name for the engine parameter for defining signatures to be detected by the at least one engine.” The Office Action concedes that *Vaidya* did not disclose the above limitations. See Office Action, Page 17. Rather, the Office Action points to *Bardsley* at Paragraphs 24-30, but this is incorrect. Paragraphs 24-30 generally describe a structure of a signature file. From this general description of a signature file, Applicants are unaware as to how the “an engine parameter and an associated name for the engine parameter and user-defined signatures with parameter-value pairs associated with the user-defined signatures and an engine parameter and an associated name for the engine parameter for defining signatures to be detected by the at least one engine” could be disclosed. And, the PTO has not pointed to the particular portion relied upon in these paragraphs. For at least this reason, Independent Claim 35 and its dependents should be allowed.

Applicants additionally challenge the Office Action’s alleged motivation to combine and modify features from the references, which was provided in the Office Action as follows:

This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to prevent the spread of viruses and detect the newly introduced viruses and furthermore to match the plurality of contiguous digital signal of the test file to the plurality of contiguous digital signals of the original file (column 2, lines 8-12).

(Office Action, Pages 3-4, and 6, Claim 1 and 28.)

This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to detect changes to the original computer file, where the original file has an associated protection file (column 2, lines 17-20).

(Office Action, Page 5, Claim 11.)

This would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to update recognize and detect new attacks and furthermore to update attack signature files either automatically or in accordance with user-set monitoring profiles (column 5, lines 19-21).

(Office Action, Page 14, Claim 19.)

This modification would have been obvious because person having ordinary skill in the art at the time the invention was made would have been motivated to do so in order to protect the network from any attacks and furthermore to decrease the likelihood that the intrusion detection server will fail or that troublesome queues and resulting delay will build (paragraph [001 I]).

(Office Action, Page 14, Claim 35.) This conclusory reasoning provided in each of these statements falls short of the required evidence of a motivation to combine and/or modify prior art references. *See Ex Part O'Donnell*, Appeal No. 2004-0421 (The Board found that the Examiner's reason, "it would have been within the scope of one of ordinary skill in the art to combine the teachings of [the references] to achieve further corrosion resistance," an inadequate reason as to why there is a motivation to combine the references.). In order to establish a *prima facie* rejection, at a minimum, evidence as to a motivation for a modification of one or both of the references would be necessary. The PTO has provided no such evidence.

Applicants additionally provide a reminder that the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *See, e.g., In Re Jones*, 958 F.2d 347, 351, 21 U.S.P.Q.2d 1941, 1944 (Fed. Cir. 1992) ("Conspicuously missing from this record is any evidence, other than the PTO's speculation (if that can be called evidence) that one of ordinary skill in the herbicidal art would have been motivated to make the modification of the prior art salts necessary to arrive at the claimed...salt.").

Further, "[t]he factual inquiry whether to combine references must be thorough and searching." (*In re Sang-Su Lee*, 277 F.3d 1338, 1343). "[An] examiner's conclusory statements . . . do not adequately address the issue of motivation to combine." *Id.* Furthermore, simple hindsight speculation that "it would have been obvious" to make the

proposed combination is insufficient under M.P.E.P.¹ guidelines and governing Federal Circuit case law.² Moreover, such statements and assumptions are inadequate to support a finding of motivation, which is a factual question that cannot be resolved on “subjective belief and unknown authority.”³ For at least this additional reason, Applicants submit that the Independent Claims and their dependents should be allowed.

Request for Evidentiary Support

Should any of the above asserted rejections be maintained, Applicants respectfully request appropriate evidentiary support. Additionally, if the Examiner is relying upon “common knowledge” or “well known” principles to establish the rejection, Applicants request that a reference be provided in support of this position pursuant to M.P.E.P. § 2144.03. Furthermore, to the extent that the Examiner maintains any rejection based on an “Official Notice” or other information within the Examiner’s personal knowledge, Applicants respectfully request that the Examiner cite a reference as documentary evidence in support of this position or provide an affidavit in accordance with M.P.E.P. § 2144.03 and 37 C.F.R. 1.104(d)(2).

No Waiver

All of Applicants’ arguments and amendments are without prejudice or disclaimer. Applicants reserve the right to discuss the distinctions between the applied art and the claims in a later Response or on Appeal, if appropriate. By not responding to additional statements made by the Examiner, Applicants do not acquiesce to the Examiner’s additional statements. The example distinctions discussed by Applicants are sufficient to overcome the anticipation and obviousness rejections.

¹ See, e.g., M.P.E.P. §2145 X.C. (“The Federal Circuit has produced a number of decisions overturning obviousness rejections due to a lack of suggestion in the prior art of the desirability of combining references.”).

² For example, in *In re Dembicza*, 175 F.3d 994 (Fed. Cir. 1999), the Federal Circuit reversed a finding of obviousness by the Board of Patent Appeals and Interferences, explaining that evidence of a suggestion, teaching, or motivation to combine is essential to avoid impermissible hindsight reconstruction of an applicant’s invention:

Our case law makes clear that the best defense against the subtle but powerful attraction of hindsight obviousness analysis is *rigorous application of the requirement for a showing of the teaching or motivation to combine prior art references*. Combining prior art references without evidence of such a suggestion, teaching, or motivation simply takes the inventor’s disclosure as a blueprint for piecing together the prior art to defeat patentability—the essence of hindsight.

175 F.3d at 999 (quoting *W.L. Gore & Assoc., Inv. v. Garlock, Inc.*, 721 F.2d 1540, 1553 (Fed. Cir. 1983)) (emphasis added) (citations omitted).

³ See *In re Lee*, 277 F.3d 1338, 1344 (Fed. Cir. 2002).

CONCLUSION

Applicants have now made an earnest attempt to place this case in condition for immediate allowance. For the foregoing reasons and for other apparent reasons, Applicants respectfully request full allowance of all pending Claims.

If the Examiner feels that a telephone conference or an interview would advance prosecution of this Application in any manner, please feel free to contact the undersigned attorney for Applicants at 214.953.6913.

Applicants do not believe that any fees are due. However, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTT S L.L.P.
Attorneys for Applicants



Ryan S. Loveless
Reg. No. 51,970

Date: June 27, 2006

Correspondence Address:

Customer Number: **05073**